Carnegie Mellon
Software Engineering Institute

Protecting Information Infrastructures

Rich Pethia

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This work is sponsored by the U.S. Department of Defense.

Survivable Systems Initiative

The SEI established, with DARPA sponsorship, the Computer Emergency Response Team Coordination Center in 1988.

The CERT/CC's mission is to respond to security emergencies on the Internet, serve as a focal point for reporting security vulnerabilities, serve as a model to help others establish incident response teams, and raise awareness of security issues.

Activity

Since 1988, the CERT/CC has responded to over 18,000 security incidents that have affected over 220,000 Internet sites; has worked over 1200 reported vulnerabilities, and has issued 255 advisories and bulletins. In addition, the CERT/CC has helped foster the creati[illegible] 80 other incident response t[illegible]

Initiative Goal

Ensure that appropriate *technology,* **systems** *management practices*, **and supporting *i****nfrastructures* **are used to** *resist*, *recognize* **and** *recover* **from attacks on** *networked* **systems, to** *limit damage* **and to** *ensure continuity of critical services* **in spite of successful attacks.**

Focus Areas

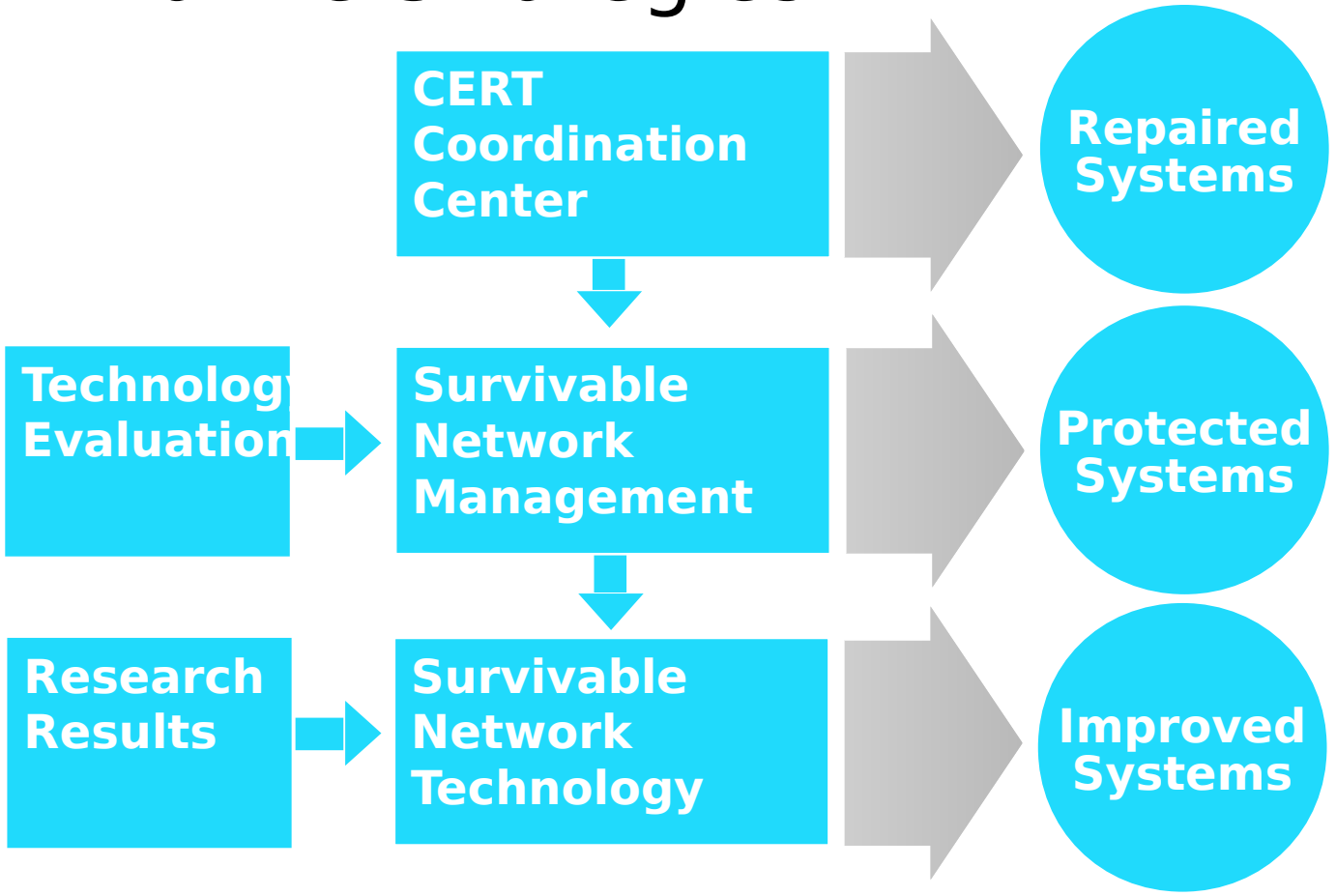
CERT/CC: Foster global security incident response and coordination by facilitating the creation of a self-sustaining incident response infrastructure.

Survivable Network Management: Establish the use of security monitoring and improvement practices and tools as routine practice by network service providers and major Internet sites.

Focus Areas - 2

Survivable Network Technology:
Reduce security incidents caused by errors in software architecture, design, or implementation.

Initiative Strategies



Why?

Networks Are Indispensable to Business

Networked systems allow organizations to:

- **conduct electronic commerce**
- **provide better customer service**
- **collaborate with partners**
- **reduce communications costs**
- **improve internal communication**
- **access needed information rapidly**

The Problem

In the rush to benefit from using networks, organizations often overlook significant security issues.

- **The engineering practices and technology used by system providers are often not sufficient to prevent the fielding of systems vulnerable to attack**
- **Network and system operators do not always follow best practices that would prevent such attacks or minimize damage**

The Risks

While computer networks revolutionize the way you do business, the risks computer networks introduce can be fatal to a business.

Network attacks lead to lost:

- **money**
- **time**
- **products**
- **reputation**
- **lives**
- **sensitive information**

Examples

Increasing damage from attacks

- **high technology bank robbery**
- **loss of intellectual property - $2M in one case**
- **extensive compromise of operational systems - 15,000 hour recovery operation in one case**
- **medical records tampering**
  - **altering results of diagnostic tests**
  - **compromising the integrity of CAT scan data**
- **extortion - demanding payments to avoid operational problems**

Strain on System Administrators

There is continued movement to complex,client-server and heterogeneous configurations with distributed management

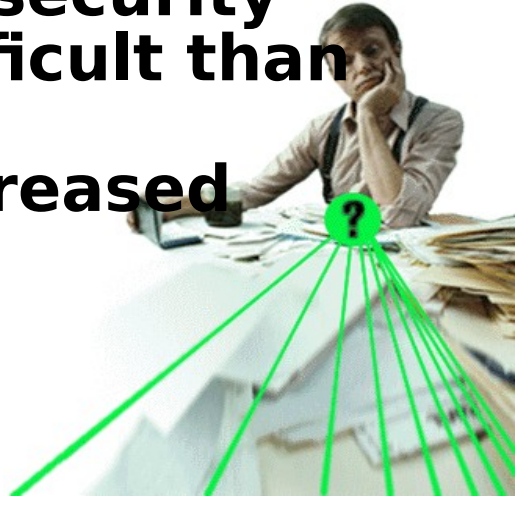
There is little evidence of security improvements in most products; new vulnerabilities are found routinely

Comprehensive security solutions are lacking; current tools address only parts of the problem

Strain on System Administrators

Engineering for ease of use has not been matched by engineering for ease of secure administration

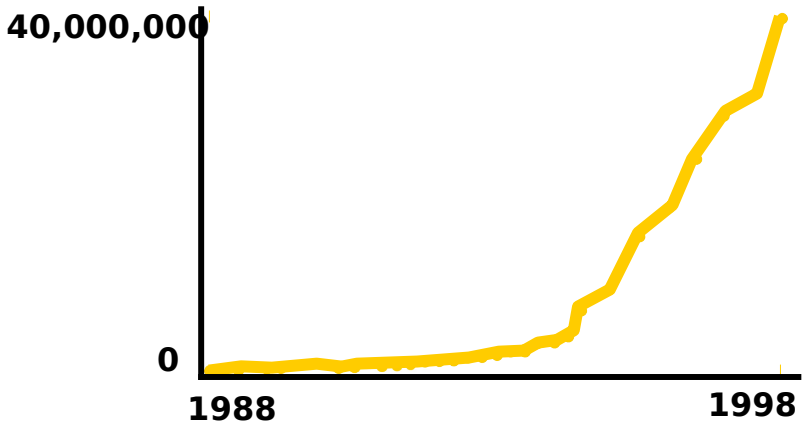
- **ease of use and increased utility are driving a dramatic explosion in use**
- **system administration and security administration are more difficult than a decade ago**
- **this growing gap brings increased vulnerability**



Yesterday's Solutions Won't Work in Today's Systems

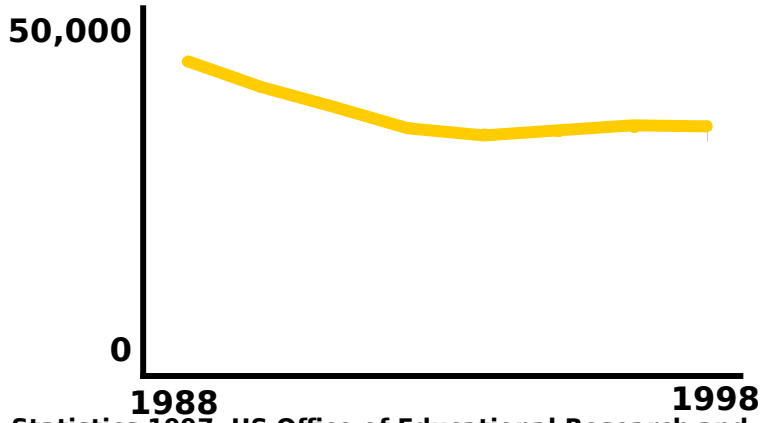
- **Open, highly distributed systems**
- **Unknown perimeters**
- **No central administrative control**
- **No global visibility**
- **Unknown components (COTS, Java, etc.)**
- **Unknown participants**
- **Untrusted insiders**
- **Large-scale coordinated attacks**

Internet Growth 1988-1998



Source: Internet Domain Survey by Network Wizards, WWW.ww.com/zone

BS and MS Degrees in Computer and Information Sciences 1988-1998



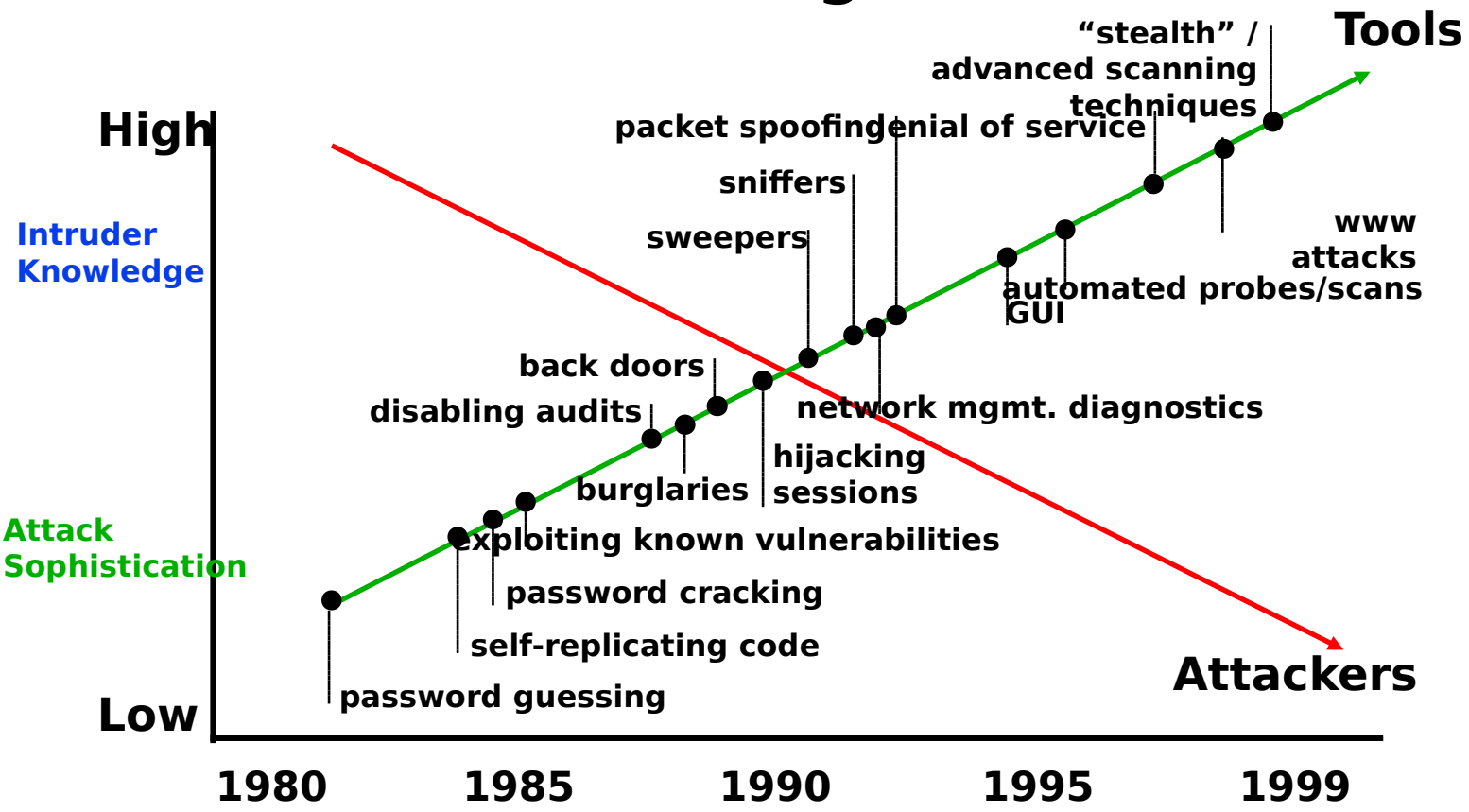
Source: Digest of Education Statistics 1997, US Office of Educational Research and Improvement,
Washington DC, publisher: US Superintendent of Document, 1997

More Sophisticated Intruders

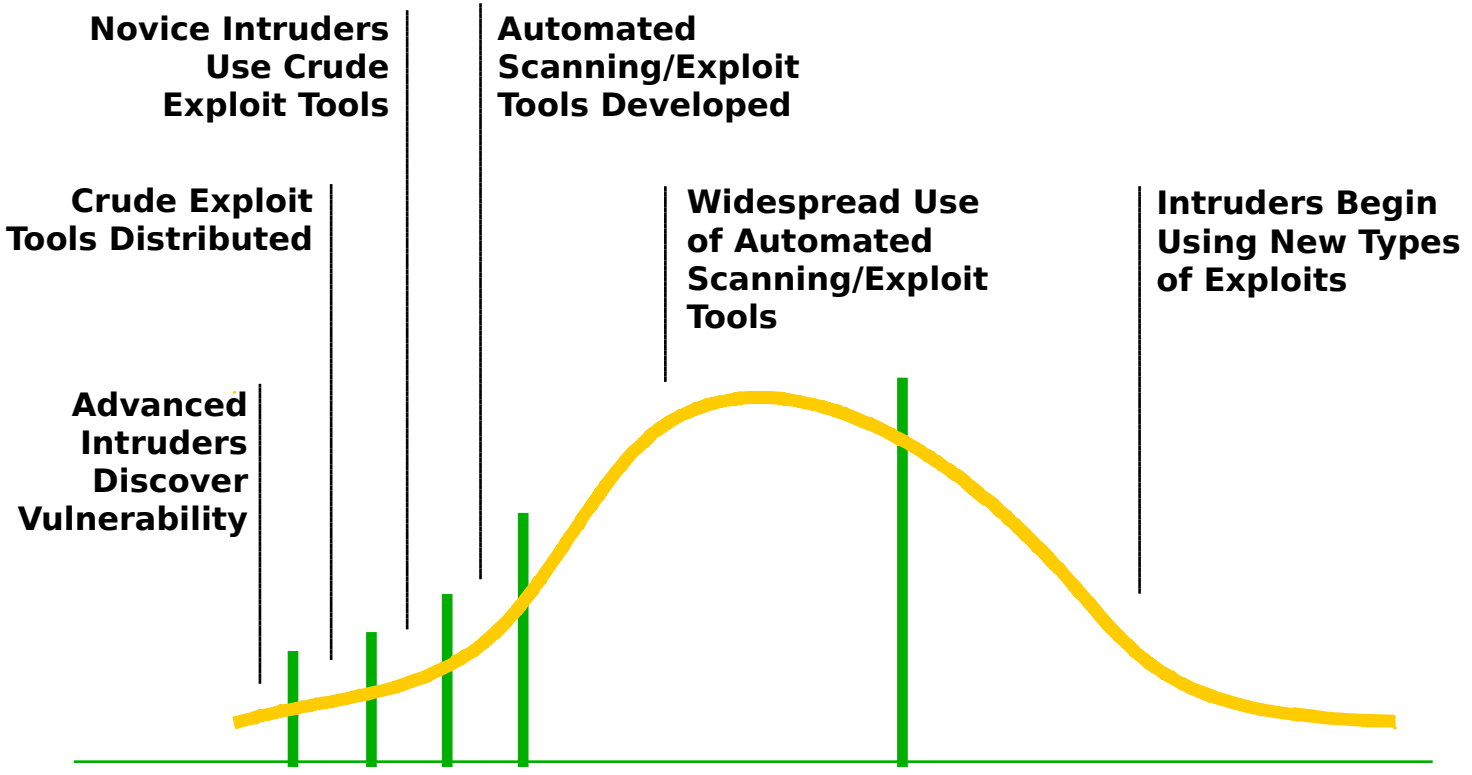
Intruders are

- **building technical knowledge and skills**
- **gaining leverage through automation**
- **exploiting network interconnections and moving easily through the infrastructure**

Attack Sophistication vs. Intruder Technical Knowledge



Vulnerability Exploit Cycle



So What?

Its going to get worse

Explosive growth of the Internet continues

- **continues to double in size every 10-12 months**
- **where will all the capable system administrators come from?**

Market growth will drive vendors

- **time to market, features, performance, cost are primary**
- **"invisible" quality features such as security are secondary**

Its going to get worse

More sensitive applications connected to the Internet

- **low cost of communications, ease of connection, and power of products engineered for the Internet will drive out other forms of networking**
- **hunger for data and benefits of electronic interaction will continue to push widespread use of information technology**

Its going to get worse

The death of the firewall

- **traditional approaches depend on complete administrative control and strong perimeter controls**
- **today's business practices and wide area networks violate these basic principles**
  - **no central point of network control**
  - **more interconnections with customers, suppliers, partners**
  - **more network applications**
    - **"the network is the computer"**
  - **who's an "insider"and who's an "outsider"**

Its going to get worse

Beware of snake-oil

- **the market for security products and services is growing faster than the supply of *quality* product and service providers**
- **an informed consumer base needs understanding, not just awareness**
- **sometimes the suppliers don't understand either**
- **"if you want it badly, you'll get it badly"**

Before it gets better

Strong market for security professionals will eventually drive graduate and certificate programs

Increasing understanding by technology users will build demand for quality security products; vendors will pay attention to the market

Insurance industry will provide incentives for improved business security practices

Before it gets better

Technology will continue to improve and we will figure out how to use it

- **encryption**
- **strong authentication**
- **survivable systems**

Increased collaboration across government and industry

CERT Contact Information

24-hour hotline:

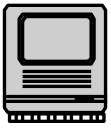
+1 412 268 7090
CERT personnel answer 8:30 a.m. — 8:00 p.m. EST(GMT-5) / EDT(GMT-4), and are on call for emergencies during other hours.

Fax:

+1 412 268 6989

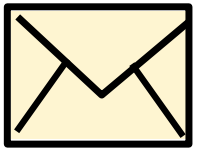
Anonymous FTP archive: **ftp://info.cert.org/pub/**
Web site: **http://www.cert.org/**

Electronic mail:



cert@cert.org

US mail:



CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213-3890
USA